***DRAFT***

NIST Special Publication 800-xx

# Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

*Recommendations of the National Institute of Standards and Technology*

U.S. DEPARTMENT OF COMMERCE

Technology Administration

National Institute of Standards and Technology

Edward A. Roback

## COMPUTER SECURITY

*Comments may be sent to* Assurance@nist.gov *and are requested by May 1, 2000.*

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 074-0188*



| 1. AGENCY USE ONLY (Leave blank) | 2. REPORT DATE | 3. REPORT TYPE AND DATES COVERED |
|---|---|---|
| | 3/20/00 | Report |

**4. TITLE AND SUBTITLE**
Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

**5. FUNDING NUMBERS**

**6. AUTHOR(S)**
Edward Roback

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

**11. SUPPLEMENTARY NOTES**

**12a. DISTRIBUTION / AVAILABILITY STATEMENT**

**12b. DISTRIBUTION CODE**
A

**13. ABSTRACT** ***(Maximum 200 Words)***

This document provides guidelines for Federal organizations' acquisition and use of security-related Information Technology (IT) products. NIST's advice is provided in the context of larger recommendations regarding security assurance.

**14. SUBJECT TERMS**
Security,Assurance

**15. NUMBER OF PAGES**

**16. PRICE CODE**

| 17. SECURITY CLASSIFICATION OF REPORT | 18. SECURITY CLASSIFICATION OF THIS PAGE | 19. SECURITY CLASSIFICATION OF ABSTRACT | 20. LIMITATION OF ABSTRACT |
|---|---|---|---|
| Unclassified | UNCLASSIFIED | UNCLASSIFIED | None |

# Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

## *Recommendations of the National Institute of Standards and Technology*

### Purpose

This document provides guidelines for Federal organizations' acquisition and use of security-related Information Technology (IT) products. NIST's advice is provided in the context of larger recommendations regarding security assurance.

### Authority

This document has been developed by NIST in furtherance of its statutory responsibilities (under the Computer Security Act of 1987 and the Information Technology Management Reform Act of 1996, specifically 15 U.S.C. 278 g-3(a)(5) ). This is not a guideline within the meaning of (15 U.S.C. 278 g-3 (a)(3)).

### Applicability

These guidelines are for use by Federal organizations which process sensitive information.[1] They are consistent with the requirements of OMB Circular A-130, Appendix III.

The guidelines herein are not mandatory and binding standards. This document may be used by non-governmental organizations on a voluntary basis. It is not subject to copyright.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding upon Federal agencies by the Secretary of Commerce under his statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, the Director of the Office of Management and Budget, or any other Federal official.

### Background

[1] Many people think that sensitive information only requires protection from unauthorized disclosure. However, the Computer Security Act provides a much broader definition of the term "sensitive information:" *any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.*

These guidelines provide advice to agencies *for sensitive (i.e., non-national security) unclassified systems*. This advice regarding sensitive unclassified systems complements the guidance recently issued for the *national security* community for the use and acquisition of "information assurance" products.

In January 2000, the National Security Telecommunications and Information Systems Security Committee (NSTISSC) issued National Security Telecommunications and Information Systems Security Policy (NSTISSP) Number 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products." NSTISSP Number *11 applies to national security systems* as defined in National Security Directive 42. A summary of NSTISSP Number 11 appears in Appendix II for reference purposes. The complete document is available to Government organizations through the NSTSSC Secretariat (I42), National Security Agency, 9800 Savage Road, Ft. Meade, MD, 20755-6716.

## Guidelines

### 1. Federal departments and agencies should understand the concept of computer security assurance.

Broadly speaking, computer security assurance provides a basis for one to have confidence that security measures, both technical and operational, work as intended. Varying degrees of assurance are supported through methods such as conformance testing, security evaluation, and manufacturer's published assertions. Assurance is not, however, a guarantee that the measures work as intended; it is closely related to areas of reliability and quality.[2]

### 2. Federal departments and agencies should be aware of how assurance in the acquired products supports security.

In general, the higher the assurance, the greater the confidence a manager has that the IT products, systems, networks being used work as intended and are being sufficiently protected.[3] Assurance in individual product components contributes to overall system security assurance – but it neither provides a guarantee of system assurance nor, in and of itself, secures a system. Use of products with an appropriate degree of assurance contributes to security and assurance of the system as a whole and thus should be an important factor in IT procurement decisions. For a security product, system or software a combination of measures for such areas as security functionality, sound development and operational practices, and periodic inspection and review needs to be addressed as well. In other words, complementary and interdependent controls are needed, such as

[2] Details regarding the definition of assurance and some means for obtaining can be found in NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook" available at http://csrc.nist.gov/nistpubs/.

[3] Sufficient protection refers to the level of security deemed so by the management official who authorization of a system to process information, (some agencies refer to this authorization as accreditation). See Appendix III to OMB Circular A-130.

sound operating procedures, adequate training, comprehensive policies, sound security architectures, and a comprehensive risk management program.

**3. Federal departments and agencies should be knowledgeable of the many approaches to obtaining security assurance in the products they procure.**

There are a number of ways that security assurance in products and systems is supported, such as:

NIST, NSA or other Conformance Testing and Validation Suites
Testing and Certification
Evaluation and Validation
Advanced or Trusted Development Techniques
Warranties, Integrity Statements, and Liabilities
Manufacturer's Published Assertions
Secure Distribution

See Chapter 9 entitled "Assurance" in *An Introduction to Computer Security: The NIST Handbook NIST Computer Security Handbook* and the Common Criteria general information web page at *http://csrc.nist.gov/nistpubs/ and http://csrc.nist.gov/cc/info/infolist.htm*, for a fuller discussion.

**4. Federal agencies should specifically be aware of the security assurance benefits, which can be obtained though testing of commercial products against customer, government, or vendor-developed specifications.**

Two Government programs are of particular interest here – the National Information Assurance Partnership (NIAP)'s Common Criteria Evaluation and Validation Program and NIST's Cryptographic Module Validation Program (CMVP). The NIAP program focuses on *evaluations* of products (e.g., a firewall or operating system) against a set of security specifications. The CMVP program focuses on security *conformance testing* of a cryptographic module against Federal Information Processing Standard 140-1, *Security Requirements for Cryptographic Modules* and related Federal cryptographic algorithm standards.

The **NIST / NSA – sponsored NIAP** is a U.S. Government initiative designed to meet the security evaluation needs of both IT producers and consumers. The program is intended to foster the availability of objective methods for evaluating the quality of IT security products. In addition, NIAP is designed to foster the development of commercial testing laboratories that can provide the types of testing and evaluation services which will meet the demands of both producers and users. The NIAP focuses on evaluations conducted in accordance with the "Common Criteria" (ISO 15408) evaluation approach. The "Common Criteria" specified seven predefined assurance packages, known as Evaluation Assurance Levels (EALs), as described in Appendix I. Agencies may use the laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) to perform evaluations of products against specifications expressed using the

"Common Criteria." As the NIAP progresses, such specifications, known as "protection profiles" will be developed by industry and government consumers. For those specifications which may be appropriate to a broad segment of its Federal community, NIST intends to generally promulgate protection profiles as technical guidelines to the Federal community following an informal agency review and comment process. Testing can also be accomplished against vendor-developed security requirements associated with a vendor's specific product or system, known as a "security target." This testing can support vendor security claims. The evaluation conducted by accredited private sector laboratories under the auspices of NIAP provides for varying levels of assurance, to meet customer requirements. (See http://niap.nist.gov.)

The **Cryptographic Module Validation Program** (CMVP), which is jointly run with the Government of Canada's Communications Security Establishment, helps provide customers with assurance that:

1) a cryptographic module meets one of the four security specification levels of Federal Information Processing Standard 140-1, *Security Requirements for Cryptographic Modules* (a mandatory Federal Information Processing Standard for sensitive (unclassified) applications and

2) that the FIPS-approved algorithms (e.g., Triple DES) are correctly implemented.

Assurance of the proper functioning of cryptographic modules and algorithms is generally considered critical because encryption techniques are used to protect sensitive data that is transmitted over untrusted paths (e.g., over the Internet). Additionally, the knowledge of and consequences resulting from unauthorized disclosure of information may not be apparent for some time (as compared, say, to the immediate awareness that a homepage has been defaced). The specifications for FIPS 140-1 and a current list of validated modules can be found at http://csrc.nist.gov/cryptval/

CMVP tested modules are often integrated into commercial products with additional (i.e., non-cryptographic) functionality. The assurance provided by CMVP concerning cryptographic modules does not imply assurance with regard to other aspects of the product into which the module is incorporated.

**5. Federal departments and agencies should acquire and use products appropriate to their risk environment and their cost-effective selection of security measures. When selecting products, agencies need to consider the threat/risk environment, cost-effectiveness, assurance level, and security functional specifications, as appropriate.**

A listing of products which have been validated under the NIAP's Common Criteria Evaluation and Validation Program can be found at http://niap.nist.gov/cc-scheme/ValidatedProducts.html. At the time of this writing, no Common Criteria protection profiles have been designated as mandatory and binding by the Secretary of

Commerce. It is NIST's intent to issue protection profiles (when appropriate) as technical security guidelines to the Federal community.

With specific regard to ***cryptographic modules and FIPS-approved cryptographic algorithms***, agencies are reminded that the use of modules tested as conformant to Security Requirements for Cryptographic Modules (a Federal Information Processing Standard) has been made mandatory and binding by the Secretary of Commerce. NIST maintains a publicly available list of modules, which have been so validated. (See http://csrc.nist.gov/cryptval/.)

6. **Federal departments and agencies need to address how products (with appropriate assurance) are configured and integrated properly, securely and subject to the managerial operational approval process[4] so as to help ensure security is appropriately addressed on a system-wide basis.**

The overall assurance level of a system as a whole may be different (usually lower) than the assurance level of individual components. While product assurance is a crucial and necessary input into the system security process, all the usual policies, controls, and risk management processes must also be in place for a system to operate in a reasonably secure mode. There are typically specific configuration settings that must be employed for the product to operate in the secure manner desired. In addition, much attention must be paid to combining such products in order to provide an appropriate security solution for a given risk and threat environment. Thus, in addition to employing products with appropriate security capabilities and assurance, review of the security of a system from a system-side perspective supports the managerial operational approval process.

Agencies should also be aware of the interconnectivity and associated interdependence of organizations and that a risk accepted by one organization may inadvertently expose other organizations to the same risk.

**Supplemental Information**

**Appendix I:** Common Criteria Evaluation Assurance Levels, reproduced from "Common Criteria 2 An Introduction," a brochure produced by Syntegra on behalf of the Common Criteria Project Sponsoring Organizations. (Its development was sponsored in part by NIST.)

The following two documents, issued by the National Security Telecommunications and Information Systems Security Committee are *applicable to national security systems*, are reproduced here for information purposes. *Note: Appendices II and III are not included in this electronic draft.*

**Appendix II:** *Fact Sheet -- National Security Telecommunications and Information Systems Security (NSTISSP) Number 11, National Information Assurance Acquisition*

[4] This refers to the approval process discussed in Office of Management and Budget Circular A-130, Appendix III.

*Policy*. (NSTISSP Number 11 itself is "For Official Use Only" and therefore not included in this document.)

**Appendix III:** *National Security Telecommunications and Information Systems Security Committee Advisory Memorandum for the Strategy for Using the National Information Assurance Partnership (NIAP) for the Evaluation of Commercial Off-the-Shelf (COTS) Security Enabled Information Technology Products*. (NSTISSAM INFOSEC/2-00)

## Appendix I

## Common Criteria Evaluation Assurance Levels [5]

The CC has provided seven predefined assurance packages, known as Evaluation Assurance Levels (EALs). These provide balanced groupings of assurance components that are intended to be generally applicable. The seven EALs are as follows:

EAL1 - functionally tested
EAL2 - structurally tested
EAL3 - methodically tested and checked
EAL4 - methodically designed, tested and reviewed
EAL5 - semiformally designed and tested
EAL6 - semiformally verified design and tested
EAL7 - formally verified design and tested

**Evaluation Assurance Level**
Each of the seven Evaluation Assurance Levels is summarized below. EAL1 is the entry level. Up to EAL4 increasing rigour and detail are introduced, but without introducing significant specialized security engineering techniques. EAL1-4 can generally be applied to products and systems not developed with evaluation in mind. Above EAL4 the increasing application of specialized security engineering techniques is required. TOEs meeting the requirements of these levels of assurance will most likely have been designed and developed with the intent of meeting those requirements. At the top level (EAL7) there are significant limitations on the practicability of meeting the requirements, partly due to substantial cost impact on the developer and evaluation activities, and also because anything other than the simplest of products is likely to be too complex to submit to state of the art techniques for formal analysis.

**EAL1** EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information. This level provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided.

**EAL2** EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require

[5] This Appendix is reproduced from "Common Criteria 2 An Introduction," a brochure produced by Syntegra on behalf of the Common Criteria Project Sponsoring Organizations. (Its development was sponsored in part by NIST.)

a substantially increased investment of cost or time. EAL2 is applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.

**EAL3** EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices. It is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without incurring substantial re-engineering costs. An EAL3 evaluation provides an analysis supported by "gray box" testing, selective confirmation of the developer test results, and evidence of a developer search for obvious vulnerabilities. Development environment controls and TOE configuration management are also required.

**EAL4** EAL4 permits a developer to maximize assurance gained from positive security engineering based on good commercial development practices. Although rigorous, these practices do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. It is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs, and are prepared to incur additional security-specific engineering costs.

An EAL4 evaluation provides an analysis supported by the low-level design of the modules of the TOE, and a subset of the implementation. Testing is supported by an independent search for vulnerabilities. Development controls are supported by a life-cycle model, identification of tools, and automated configuration management.

**EAL5** EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialized techniques, will not be large. EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques. An EAL5 evaluation provides an analysis that includes all of the implementation. Assurance is supplemented by a formal model and a semiformal presentation of the functional specification and high-level design, and a semiformal demonstration of correspondence. The search for vulnerabilities must ensure resistance to attackers with a moderate attack potential. Covert channel analysis and modular design are also required.

**EAL6** EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks. EAL6 is therefore applicable to the development of security TOEs for application in high-risk situations where the value of the protected assets justifies the additional costs. An EAL6 evaluation provides an analysis that is supported by a modular and layered approach to design, and a structured presentation of the implementation. The independent search for vulnerabilities must ensure resistance to attackers with a high attack potential. The search for covert channels must be systematic. Development environment and configuration management controls are further strengthened.

**EAL7** EAL7 is applicable to the development of security TOEs for application in extremely high-risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis. For an EAL7 evaluation the formal model is supplemented by a formal presentation of the functional specification and high-level design, showing correspondence. Evidence of developer "white-box" testing and complete independent confirmation of developer test results are required. Complexity of the design must be minimized.

*Note: Appendices II and III are not included in this electronic draft.*